ISE RADIUS-Kontextauslastung bewirkt, dass der Knoten nicht mehr reagiert

Inhalt

Problem

Ein Cisco Identity Services Engine (ISE)-Knoten reagiert gelegentlich nicht mehr auf RADIUS-Authentifizierungsanforderungen, sodass Netzwerkgeräte ihn als "RADIUS DEAD" markieren. Der betroffene Knoten empfängt RADIUS-Anfragen (bestätigt durch Firewall-Protokolle und Paketerfassung), reagiert aber nicht. Folgende Symptome wurden beobachtet:

- RADIUS-Nachrichten zur erneuten Übertragung auf Netzwerkgeräten
- "Radius Context Allocation Failed" (RADIUS-Kontextzuweisung fehlgeschlagen) - kritische Alarme in ISE
- Protokollieren Sie Meldungen, die den Grenzwert für die Anzahl der Treffer im Kontext angeben. Anfrage wird gelöscht!"
- Auf die ISE-GUI kann während des Problems nicht zugegriffen werden, obwohl alle Dienste als ausgeführt angezeigt werden
- Knoten startet neu und löst das Problem vorübergehend für ca. 30 Minuten, bevor es erneut auftritt

Folgende Fehlermeldungen wurden beobachtet:

```
033057: Mar 11 09:33:59.015: RADIUS: Retransmit to (10.0.5.11:1812,1813) for id 1645/127
033058: Mar 11 09:33:59.015: RADIUS: PAC key found while sending request (rctx:0x75EB6A555690)
033059: Mar 11 09:33:59.015: RADIUS: Message Authenticator encoded
033060: Mar 11 09:33:59.015: RADIUS(00000000): Started 4 sec timeout
```

Und in ISE-Protokollen:

```
RadiusListener,2026-06-28 23:21:22,149,WARN ,0x7efea2055700,NIL-CONTEXT,Hit context count limit. Droppi
```

Umwelt

- Cisco Identity Services Engine (ISE) Version 3.5.0.331 (Patch 3)
- Knoten für mehrere Rollen: Primary Administration Node (PAN), Session Management and Troubleshooting (SMNT) und Policy Service Node (PSN)
- Authentifizierungsmethoden: 802.1X- und MAB-Unterstützung an Access Switch-Ports
- Externe Identitätsquellen: Microsoft Entra ID-Integration
- Netzwerkgeräte, die mit ISE als RADIUS-Server für die Authentifizierung konfiguriert sind

Auflösung

Das Problem wurde durch die Anwendung eines von Cisco bereitgestellten Hotfix behoben, der eine Deadlock-Bedingung im ISE SessionUpdater-Prozess behebt. Befolgen Sie diese Schritte, um die Entschließung umzusetzen:

Schritt 1: Abrufen und Installieren des Hotfix

Laden Sie die Hotfix-Dateien von Cisco herunter, und übertragen Sie sie in Ihr ISE-Knoten-Repository. Die Hotfix-Dateien sind:

- ise-apply-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz (Installationsdatei)
- ise-rollback-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz (Rollbackdatei)

Phase 2: Hotfix anwenden

Installieren Sie den Hotfix mithilfe des CLI-Befehls:

```
application install ise-apply-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz <repository name>
```

⚠Vorsicht: Möglich. Die hier genannten Details enthalten offenbar Prozeduren oder Befehle, die bei ihrer Ausführung erhebliche Auswirkungen haben könnten. Stellen Sie sicher, dass die oben genannten Verfahren oder Befehle von einem SME oder einem Geschäftsbereich evaluiert wurden, bevor Sie sie ausführen oder empfehlen.

Schritt 3: Installation überprüfen

Überprüfen Sie die Hotfix-Installation mit einem der folgenden Befehle:

```
show logging application hotpatch.log
```

ODER:

```
show version
```

Schritt 4: Überwachen des Systems

Überwachen Sie den ISE-Knoten nach der Installation mindestens zwei Wochen, um sicherzustellen, dass das Problem nicht erneut auftritt. Die Hotfix-Installation erfordert einen Neustart des Dienstes. Planen Sie daher die Installation während eines Wartungsfensters.

Optional: Rollback-Prozedur

Bei Bedarf kann der Hotfix mit dem Befehl rollback entfernt werden:

```
application install ise-rollback-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz <repository name>
```

Fehlerbehebungsbefehle für die Überwachung

Um die RADIUS-Kontextzuweisung zu überwachen, verwenden Sie:

```
show logging application prrt-server.log | include ContextN
```

Aktivieren Sie die AAA-Laufzeitdebugging vor jeder zukünftigen Fehlerbehebung:

```
debug aaa runtime
```

Ursache

Die Ursache wurde im ISE SessionUpdater-Prozess als Deadlock-Bedingung identifiziert. Wenn das Starten und Beenden der gleichzeitigen Abrechnung für dieselbe Sitzung aufgetreten ist, haben zwei Threads in ein zirkuläres Warteszenario eingetreten:

- Thread-162: Zugeordneter cacheLock, auf Sitzungsinfo-Sperre gewartet
- Thread-125: Eigene SessionInfo-Sperre, auf cacheLock gewartet

Dieses zirkuläre Warten führte zu ContextN-Lecks und einer ständig wachsenden RADIUS-Verarbeitungswarteschlange. Durch die Warteschlangeneinrichtung wurden schließlich die verfügbaren RADIUS-Kontexte erschöpft, wodurch die Authentifizierungslatenz und die Netzwerkgeräte den ISE-Knoten als RADIUS DEAD markierten.

Das Problem ist in der Cisco Bug-ID CSCwv71473 dokumentiert.

Verwandte Inhalte

- Cisco Bug-ID: CSCwv71473
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.